From: Aliber, Jon [Jon.Aliber@fmr.com]
Sent: Friday, January 19, 2007 2:36 PM
To: Taskforcecomments
Subject: Identify Theft Task Force Comments

Picture (Metafile)

January 19, 2007

(Via E-mail: Taskforcecomments@IDTheft.gov)

Identity Theft Task Force
Federal Trade Commission
Office of the Secretary
Room H-135 (Annex N)
600 Pennsylvania Avenue, N.W.
Washington, DC 20580

To Whom It May Concern:

Fidelity Investments appreciates the opportunity to comment on the efforts of the Identity Theft Task Force. Fidelity Investments is the largest mutual fund company in the United States and is one of the largest providers of financial services with more than 22 million customers and more than $2.8 trillion under management and custody.

While we have broader comments to the task force related to the entire strategic plan that will be incorporated in comments from trade associations and coalitions in which we participate, we would like to highlight one issue of particular concern that responds generally to Issue I (Maintaining Security of Consumer Data) and Issue II (Preventing the Misuse of Consumer Data).

Fidelity Investments, as a matter of conducting its varied businesses, is required by law and regulation to send files and transmissions containing consumer data to various government authorities. This transfer of information may occur at regular intervals (e.g. monthly, annually) or due to ad hoc requests associated with regulatory reviews or other governmental needs. Examples of data transfers include reporting to tax authorities, including the Internal Revenue Service and state and local revenue authorities, for the vast majority of Fidelity's customers. Other federal agencies to which Fidelity regularly sends data are the Department of Labor, the Social Security Administration and the Securities and Exchange Commission. In many cases, federal law and regulation require us to transmit sensitive non-public personal information.

In all of our businesses, Fidelity has consistently made protection of customer data a high priority to uphold the trust our customers place in us. We have taken extensive concrete steps to protect the data we hold by establishing appropriate administrative, technical, and physical safeguards. We generally use encryption to safeguard transmission of non-public personal information. Unfortunately, unlike many private sector firms, federal and state agencies are generally unable to accept encrypted information from Fidelity. Consequently, in order to comply with many of the federal mandates to provide information, we must transfer required customer data to the government in unencryped form. This inability to accept encrypted data presents a risk to customers of all companies that must submit electronic information to the government. This risk could be avoided by adoption by governmental agencies of appropriate encryption procedures.

Fidelity respectfully urges that the task force should include in its recommendations a statement recognizing the need for government to develop options for obtaining the capacity to receive encrypted data consistently across federal agencies.

Sincerely,

Jonathan Aliber
Executive Vice-President, Chief Information Security Officer
Fidelity Investments
82 Devonshire St. V8A
Boston, MA 02109